

510 Broadway • P.O. Box 136
Abercrombie, ND 58001

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 29, 2009

Name of company covered by this certification: Red River Rural Telephone Association

Form 499 Filer ID: 807012

Name of signatory: Jeffrey J. Olson

Title of signatory: Executive Secretary/General Manager

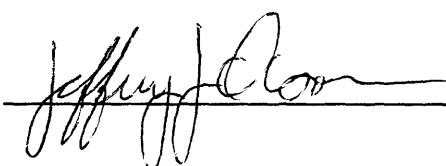
I, Jeffrey J. Olson, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. See *attached accompanying statement of operating procedures.*

The Company has not taken any actions (proceedings instituted or petitions filed by a Company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The Company currently has no information with respect to the processes pretexters are using to attempt to access CPNI. At this time, we have not encountered known pretexting. Our protective measures against pretexters are outlined in the accompanying statement of operating procedures.

Signed: 

"Your Total Communications Company ~ Connecting You To The World"

Phone 701-553-8309 • Fax 701-553-8396

Attachment: Accompanying Statement of Operating Procedures

Per the FCC CPNI rules [47 CFR §64.2009(e)] and as referenced in the attached signed certification, Red River Rural Telephone Association, herein referenced as the Company hereby certifies that the Company is in compliance with the FCC CPNI rules and has outlined some of the important operating procedures below in order to ensure the Company's compliance in the protection of CPNI:

1. CPNI manual has been updated in order to account for all FCC CPNI rules, including the recent revisions, and has been adopted by our Company's Board of Directors.
2. CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity.
 - CPNI is not utilized for marketing purposes.
3. Employees have been trained on when they are, and are not, authorized to use or disclose CPNI.
 - Disciplinary process has been defined and is in place for violations and/or breaches of CPNI.
4. Carrier authentication requirements have been met.
 - All customers during a customer-initiated telephone call are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC.
 - Call detail is only released to customers during customer-initiated telephone contact if a password is provided. However, if the customer or authorized contact does not have the password, backup authentication procedures using security questions are followed. If the requesting customer does not provide a password or backup authentication, only the following FCC approved methods are permitted for the release of the requested call detail:
 - Sending the requested detail to the address of record (only a physical or e-mail address associated with that particular account that has been in our company files for at least 30 days)
 - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
 - Having customer come in to Company's office and provide a valid government issued photo ID.
5. Notice to customer of account change - customers are notified immediately when a customer creates or changes one of the following:
 - password
 - customer response to a back-up means of authentication for lost or forgotten passwords
 - online account
 - address of record
6. Notice of unauthorized disclosure of CPNI - a notification process is in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC.
7. Additional protection measures are taken above and beyond the current FCC CPNI rules:
 - Company takes reasonable measures to discover and protect against activity that is indicative of pretexting.
 - Company maintains security of all CPNI including shredding documents containing CPNI.